BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-355266
(43)Date of publication of application : 24.12.1999

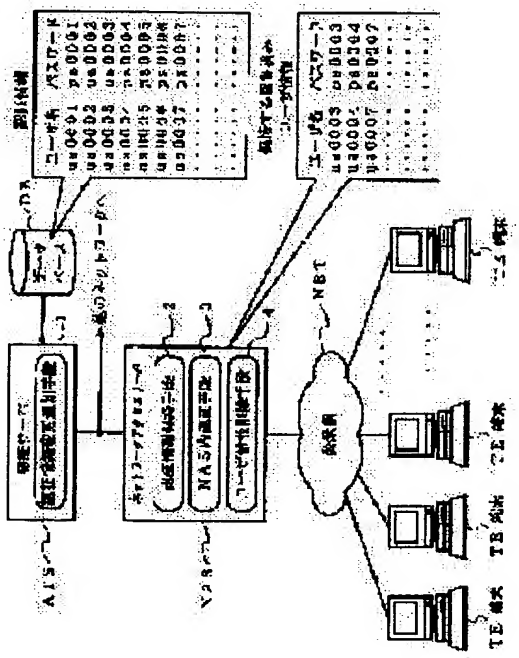
(51)Int.Cl. H04L 9/32
G06F 15/00

(21)Application number : 10-157079
(22)Date of filing : 05.06.1998

(71)Applicant : NEC CORP
NEC TELECOM SYST LTD
(72)Inventor : WATANABE NATSUKO
TERAKADO MASASHI

(54) DEVICE AND METHOD FOR USER AUTHENTICATION

(57)Abstract:
PROBLEM TO BE SOLVED: To reduce a load on a server which performs user authentication in accessing other networks and to simplify the system structure.
SOLUTION: An authentication information holding means 2 holds what is authenticated by an authentication server ATS as authenticated user information among the authentication information which a database DB stores. When a user accesses other networks from a terminal TE, if the terminal TE is dial- up-connected to a network access server NAS, an authentication demand including a user name and a password is made by the terminal TE of the NAS. An in-NAS authentication means 3 retrieves whether or not the user name and the password are held by the authentication information holding means 2, 'authenticated' when the two coincide with each other or 'authentication denied' when the password does not coincide is replied to the terminal TE. Also, when the user name concerned does not exist, the authentication is demanded of the authentication server ATS. When the authentication server ATS finds the user name concerned in the database DB, it responds with fulfilled authentication to the NAS and the terminal, and holds its user name and the password in the authentication information holding means 2.



LEGAL STATUS

[Date of request for examination] 05.06.1998
[Date of sending the examiner's decision of rejection] 13.11.2001
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－355266

(43)公開日　平成11年(1999)12月24日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７５Ｄ
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｂ
		Ｈ０４Ｌ　9/00	６７３Ａ

審査請求　有　　請求項の数９　ＯＬ　（全８頁）

(21)出願番号　特願平10－157079

(22)出願日　平成10年(1998)６月５日

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号

(71)出願人　000232106
日本電気テレコムシステム株式会社
神奈川県川崎市中原区小杉町１丁目403番地

(72)発明者　渡邊　夏子
東京都港区芝五丁目７番１号　日本電気株式会社内

(72)発明者　寺門　雅司
神奈川県川崎市中原区小杉町一丁目403番地　日本電気テレコムシステム株式会社内

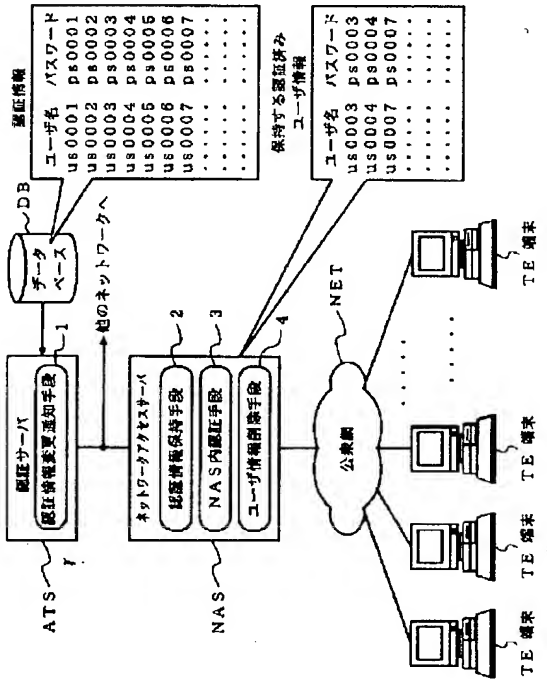
(74)代理人　弁理士　岩佐　義幸

(54)【発明の名称】　ユーザ認証装置およびユーザ認証方法

(57)【要約】

【課題】　他のネットワークへアクセスするときのユーザ認証を行うサーバの負荷を低減し、かつシステム構成を単純化する。

【解決手段】　認証情報保持手段２は、データベースＤＢが格納する認証情報中、認証サーバＡＴＳによって認証されたものを認証済みユーザ情報として保持している。ユーザが端末ＴＥから他のネットワークへアクセスするときは、端末ＴＥがネットワークアクセスサーバＮＡＳにダイヤルアップ接続すると、端末ＴＥからＮＡＳへユーザ名およびパスワードを含む認証要求をする。ＮＡＳ内認証手段３は、そのユーザ名およびパスワードが認証情報保持手段２に保持されているか否かを検索し、両者一致の場合は「認証」、パスワード不一致の場合は「認証拒否」を端末ＴＥに応答する。また、該当するユーザ名が存在しないときは、認証サーバＡＴＳに認証要求する。認証サーバＡＴＳがデータベースＤＢ内に該当するユーザ名を発見すれば、ＮＡＳと端末に認証応答するとともに、認証情報保持手段２にそのユーザ名とパスワードを保持する。



1

【特許請求の範囲】

【請求項１】公衆回線網に接続された端末からルーターを介して接続された他のネットワークにアクセスするときにユーザの認証を行うユーザ認証装置において、認証済みユーザ認証情報を前記ルーターに記憶しておき、該認証済みユーザ認証情報を用いて前記ユーザの認証を行うことを特徴とするユーザ認証装置。

【請求項２】前記ルーター配下の端末を使用するユーザの認証情報を格納するデータベースと、該データベースをアクセスして前記ユーザの認証を行う認証サーバと、前記認証済みユーザ認証情報を保持する認証情報保持手段および前記ユーザの認証は先ず前記保持するユーザ認証情報を用いて行うＮＡＳ内認証手段を含み前記ルーターとして機能するネットワークアクセスサーバとを有し、前記認証サーバによるユーザの認証は、前記認証情報保持手段に該当する認証済みユーザ認証情報が保持されていないときにのみ行うことを特徴とする請求項１記載のユーザ認証装置。

【請求項３】前記認証サーバは、データベースに格納するユーザ認証情報が変更されるとその通知を行う認証情報変更通知手段を有し、また、前記ネットワークアクセスサーバは、前記通知を受けると前記保持する認証済みユーザ認証情報のうちから該当するものを削除するユーザ情報削除手段を有することを特徴とする請求項２記載のユーザ認証装置。

【請求項４】前記ユーザ情報削除手段に代えて、前記通知を受けると前記保持するユーザ認証情報のうちから該当するものを変更するユーザ情報変更手段を設けたことを特徴とする請求項３記載のユーザ認証装置。

【請求項５】前記認証情報保持手段は、所定期間内に認証要求を受けなかった認証済みユーザ認証情報を破棄することを特徴とする請求項２～請求項４のいずれかに記載のユーザ認証装置。

【請求項６】前記認証情報保持手段は、保持する認証済みユーザ認証情報が所定件数に達するとそれ以上の認証済みユーザ認証情報は破棄することを特徴とする請求項２～請求項４のいずれかに記載のユーザ認証装置。

【請求項７】前記破棄は保持の古い順に行うことを特徴とする請求項６記載のユーザ認証装置。

【請求項８】公衆回線網に接続された端末から、ルーターを介して接続された他のネットワークにアクセスするときにユーザの認証を行うユーザ認証方法において、前記ルーター配下の端末を使用するユーザの認証情報をデータベースに格納する手順と、該データベースをアクセスしてユーザの認証を行う手順と、認証済みユーザ認証情報を前記ルーターに保持する手順と、前記ユーザの認証は先ず前記ルーターに保持する認証済みユーザ認証情報を用いて行う手順と、該保持する認証済みユーザ認証情報に該当するものが無いときにのみ前記データベースアクセスによるユーザの認証を行う手順とを含むことを

2

特徴とするユーザ認証方法。

【請求項９】前記データベースに格納するユーザ認証情報が変更されると前記保持する認証済みユーザ認証情報のうちの該当するものを削除または変更する手順を含むことを特徴とする請求項８記載のユーザ認証方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ユーザ認証装置およびユーザ認証方法、特に公衆回線網に接続された端末から、ルーターを介して接続されたザ　インターネット等他のネットワークにアクセスするときに、ユーザの認証を行うユーザ認証装置およびユーザ認証方法に関する。

【０００２】

【従来の技術】近年、ネットワーク技術やＬＳＩテクノロジーの革新を背景に、ネットワーク相互間を接続した広汎なネットワークシステムが構築できるようになり、ユーザはより広域の通信が行えるようになった。しかし、その一方でネットワーク経由でコンピュータに無制限にアクセスしてくるユーザは阻止する必要がある。そのため、特にオープン・ネットワークでは、ユーザがマシンやサービスに対して利用を許可された当人であることを認証する認証システムが重要視される。

【０００３】従来のこの種のユーザ認証システムの典型的な一例を図９に示す。図９において、公衆網ＮＥＴに複数の端末ＴＥが接続されたネットワークが、ネットワークアクセスサーバＮＡＳ１を介して接続された他のネットワーク（図示省略）に結合される。データベースＤＢは、端末ＴＥを利用するユーザのユーザ名とパスワードから成る認証情報を格納しており、認証サーバＡＴＳ１は、ネットワークアクセスサーバＮＡＳ１からの認証要求によりデータベースＤＢを参照してユーザの認証を行う。ネットワークアクセスサーバＮＡＳ１はルーターの一種であり、モデムを内蔵する。

【０００４】ユーザが端末ＴＥからユーザ名とパスワードを入力して他のネットワークにアクセスしようとすると、ネットワークアクセスサーバＮＡＳ１は認証サーバＡＴＳ１に認証要求を行い、認証サーバＡＴＳ１は、入力されたユーザ名とパスワードがデータベースＤＢに格納されているか否かを調べることによりユーザの認証を行う。この結果、許されたユーザのみが所望のネットワークにアクセスできる。

【０００５】このシステムにおいては、ユーザ数およびネットワークアクセスサーバＮＡＳ１が増加した場合、ネットワークアクセスサーバＮＡＳ１－認証サーバＡＴＳ１間の認証要求／応答が増加し、認証サーバＡＴＳ１自身の負荷も増加する。そのため、ユーザ数が増加した場合にユーザ認証のレスポンスの低下等の問題が発生する。この問題は図１０に示すように認証サーバＡＴＳ１を複数台設置するシステム構成をとることにより、各認

証サーバＡＴＳ１に認証要求の負荷を分散するようにして解決を図っている。

【０００６】また、移動体無線通信の分野ではあるが、認証結果を利用する技術として、ユーザの認証結果をユーザの識別子とともに代理認証装置に記憶し、認証要求がある場合に代理認証装置に記憶された認証結果を用いてユーザの認証を行うユーザ認証方式が特開平１０－１３９５６号公報に記載されている。

【０００７】この方式は、図１１に示すように、無線端末４０が移動して、基地局例えば３０－１１から基地局３０－１２への切り替えを行う際のユーザ認証についてのものであり、基地局３０－１１等を管理する基地局管サーバ２０に代理認証装置５０を設けたものである。一度認証を受けた無線端末４が他の基地局３０－１２に接続して、再認証を受けようとするときは、無線端末４０は前回受け取った認証パスを基地局３０－１２に送信し、認証済みであることを通知する。基地局３０－１２は、この認証パスを基地局管理サーバ２０に転送し、代理認証装置５０に認証結果があれば「認証OK」を基地局３０－１２に送信し、認証結果がなければ認証サーバ１０に認証要求を転送する。

【０００８】

【発明が解決しようとする課題】しかしながら、上述した従来技術（図１０）では、システム構成が複雑になり、またユーザ認証情報のデータベース管理も煩雑になるという問題点がある。

【０００９】また、図１１に示した従来技術では、無線端末４の側で、前回受け取った認証パスを保持する必要があり、無線端末４は一度認証されたか否かを意識しなければならず煩雑であるという問題点がある。

【００１０】本発明の目的は、認証サーバの負荷を低減するユーザ認証装置およびユーザ認証方法を提供することにある。

【００１１】本発明の他の目的は、ネットワークアクセスサーバと認証サーバ間のトラヒックを低減するユーザ認証装置およびユーザ認証方法を提供することにある。

【００１２】さらに、本発明の他の目的は、システム構成とデータベース管理を簡略化するとともに、端末側の負担を軽減し、運用コストを削減したユーザ認証装置およびユーザ認証方法を提供することにある。

【００１３】

【課題を解決するための手段】本発明のユーザ認証装置は、公衆回線網に接続された端末からルーターを介して接続された他のネットワークにアクセスするときにユーザの認証を行うユーザ認証装置において、認証済みユーザ認証情報を前記ルーターに記憶しておき、該認証済みユーザ認証情報を用いて前記ユーザの認証を行うことを特徴とする。

【００１４】本発明の好ましい実施の形態としてのユーザ認証装置は、前記ルーター配下の端末を使用するユーザの認証情報を格納するデータベースと、該データベースをアクセスして前記ユーザの認証を行う認証サーバと、前記認証済みユーザ認証情報を保持する認証情報保持手段および前記ユーザの認証は先ず前記保持するユーザ認証情報を用いて行うＮＡＳ内認証手段を含み前記ルーターとして機能するネットワークアクセスサーバとを有し、前記認証サーバによるユーザの認証は、前記認証情報保持手段に該当する認証済みユーザ認証情報が保持されていないときにのみ行うことを特徴とする。

【００１５】本発明の好ましい実施の形態としてのユーザ認証装置は、前記認証サーバは、データベースに格納するユーザ認証情報が変更されるとその通知を行う認証情報変更通知手段を有し、また、前記ネットワークアクセスサーバは、前記通知を受けると前記保持する認証済みユーザ認証情報のうちから該当するものを削除するユーザ情報削除手段を有することを特徴とする。

【００１６】本発明の好ましい実施の形態としてのユーザ認証装置は、前記認証情報保持手段は、所定期間内に認証要求を受けなかった認証済みユーザ認証情報を破棄することを特徴とする。

【００１７】本発明の好ましい実施の形態としてのユーザ認証装置は、前記認証情報保持手段は、保持する認証済みユーザ認証情報が所定件数に達するとそれ以上の認証済みユーザ認証情報は破棄することを特徴とする。

【００１８】また、本発明のユーザ認証方法は、公衆回線網に接続された端末から、ルーターを介して接続された他のネットワークにアクセスするときにユーザの認証を行うユーザ認証方法において、前記ルーター配下の端末を使用するユーザの認証情報をデータベースに格納する手順と、該データベースをアクセスしてユーザの認証を行う手順と、認証済みユーザ認証情報を前記ルーターに保持する手順と、前記ユーザの認証は先ず前記ルーターに保持する認証済みユーザ認証情報を用いて行う手順と、該保持する認証済みユーザ認証情報に該当するものが無いときにのみ前記データベースアクセスによるユーザの認証を行う手順とを含むことを特徴とする。

【００１９】

【発明の実施の形態】次に、本発明の実施の形態について説明する。

【００２０】本発明のユーザ認証装置は、公衆回線網に接続された端末からルーターを介して接続された他のネットワークにアクセスするときにユーザの認証を行うユーザ認証装置において、認証済みユーザ認証情報を前記ルーターに記憶しておき、該認証済みユーザ認証情報を用いて前記ユーザの認証を行うことを特徴とする。

【００２１】また、本発明のユーザ認証方法は、公衆回線網に接続された端末から、ルーターを介して接続された他のネットワークにアクセスするときにユーザの認証を行うユーザ認証方法において、前記ルーター配下の端末を使用するユーザの認証情報をデータベースに格納す

る手順と、該データベースをアクセスしてユーザの認証を行う手順と、認証済みユーザ認証情報を前記ルーターに保持する手順と、前記ユーザの認証は先ず前記ルーターに保持する認証済みユーザ認証情報を用いて行う手順と、該保持する認証済みユーザ認証情報に該当するものが無いときにのみ前記データベースアクセスによるユーザの認証を行う手順とを含むことを特徴とする。

【００２２】以下、本発明の実施例について図面を参照して説明する。

【００２３】図１は、本発明の一実施例を示す。図１において、公衆網ＮＥＴに複数の端末ＴＥが接続されたネットワークが、ネットワークアクセスサーバＮＡＳを介して、ザ　インターネット等他のネットワーク（図示省略）に接続される。ネットワークサーバＮＡＳには認証サーバＡＴＳが接続され、認証サーバＡＴＳはデータベースＤＢをアクセスできる。データベースＤＢは、端末ＴＥを利用するユーザのユーザ名とパスワードから成る認証情報を格納しており、認証サーバＡＴＳは、ネットワークアクセスサーバＮＡＳからの認証要求によりデータベースＤＢを参照してユーザの認証を行う。

【００２４】認証サーバＡＴＳには、データベースＤＢが格納するユーザの認証情報が変更されると、ネットワークアクセスサーバＮＡＳに対して認証情報変更通知を行う認証情報変更通知手段１を設けている。

【００２５】また、ネットワークアクセスサーバＮＡＳには、認証情報保持手段２，ＮＡＳ内認証手段３およびユーザ情報削除手段４を設けている。認証情報保持手段２は、ネットワークアクセスサーバＮＡＳが、認証サーバＡＴＳからユーザを認証した旨の認証応答を受信した場合に、このユーザ名とパスワードをネットワークアクセスサーバＮＡＳ内に認証済みユーザ認証情報として保持する。また、ＮＡＳ内認証手段３は、接続した端末ＴＥから送られてくるユーザ名とパスワードにより、ネットワークアクセスサーバＮＡＳ内の認証済ユーザ情報を検索する。ユーザ名が認証済ユーザ情報内に存在した場合、端末ＴＥから送られてきたパスワードと認証済ユーザ情報内のパスワードを比較し、一致した場合、ユーザを認証した意味の結果である「認証」の結果を得、端末に対して認証応答を送信する。一致していなかった場合、ユーザの認証を拒否した意味の結果である「認証拒否」の結果を得、端末に対して認証拒否応答を送信する。ユーザ名とパスワードが認証済ユーザ情報内に存在しなかった場合には、ＮＡＳはユーザ情報が存在しない意味の結果である「ユーザ名無し」の結果を得、認証サーバＡＴＳに対して認証要求を送信する。さらに、ユーザ情報削除手段４は、認証サーバＡＴＳから認証情報変更通知で通知されたユーザ名に対応した情報を、認証情報保持手段２に保持している認証済ユーザ情報から削除する。

【００２６】次に、本実施例の動作について図２～図８を参照して説明する。図２は、本実施例のフローチャートである。先ず、ユーザが他のネットワークにアクセスするときは、端末ＴＥがネットワークアクセスサーバＮＡＳにダイヤルアップ接続をすると、端末ＴＥとネットワークアクセスサーバＮＡＳ間の認証プロトコルにより、端末ＴＥからネットワークアクセスサーバＮＡＳへユーザ名およびパスワードを含む認証要求を送出する。ネットワークアクセスサーバＮＡＳがこれを受信すると（Ｓ１）、ＮＡＳ内認証手段３により、認証情報保持手段２が保持する認証済ユーザ情報の検索を行う（Ｓ２）。その結果、「認証」の場合は端末ＴＥに認証応答を通知し（Ｓ３）、「認証拒否」の場合は端末ＴＥに認証拒否応答を通知し（Ｓ４）、「ユーザ名無し」の場合は認証サーバＡＴＳに認証要求を送出する（Ｓ５）。

【００２７】図３は、図２のＳ２におけるＮＡＳ内認証の詳細を示すフローチャートである。先ず、認証情報保持手段２が保持する認証済みユーザ情報から、受信している（Ｓ２）ユーザ名を検索し（Ｓ９）、存在すれば（Ｓ１０）、次に上記認証済みユーザ情報から、受信している（Ｓ２）パスワードを検索する（Ｓ１１）。そして、パスワードも一致すれば（Ｓ１２）「認証」とし（Ｓ１３，図２のＳ２）、パスワードが不一致なら（Ｓ１２）「認証拒否」（Ｓ１４，図２のＳ２）とする。また、Ｓ１０においてユーザ名が存在しなければ「ユーザ名無し」（Ｓ１５，図２のＳ２）とする。

【００２８】図４，図５，図６は、それぞれ「認証」，「認証拒否」，「ユーザ名無し」の場合の具体例を示す。図４においては、端末ＴＥからのユーザ名「ｕｓ０００２」，「パスワードｐｓ０００２」と認証済みユーザ情報のユーザ名「ｕｓ０００２」，「パスワードｐｓ０００２」が一致し、図５においては、ユーザ名「ｕｓ０００２」は一致するが、パスワード「ｐｓ０００２」と「ｘｙｚａｂｃ」は不一致、図６においては、ユーザ名「ｕｓ０００２」に該当するユーザ名が認証済みユーザ情報に存在しないことがわかる。

【００２９】再び図２において、認証要求送出（Ｓ５）に対する認証サーバＡＴＳからの応答を受信すると（Ｓ６）、その応答が認証応答なら（Ｓ７）、認証サーバＡＴＳからの認証情報を認証情報保持手段２に認証済みユーザ情報として保持して（Ｓ８）、端末ＴＥへ認証応答を通知し（Ｓ３），応答が認証拒否応答なら（Ｓ７），端末ＴＥへ認証応答拒否を通知する（Ｓ４）。

【００３０】図７は、認証要求（図２のＳ５および図６）を受けた認証サーバＡＴＳが、データベースＤＢをアクセスして、端末ＴＥから受信していた（図２のＳ１）ユーザ名「ｕｓ０００２」およびパスワード「ｐｓ０００２」を見つけて、ネットワークアクセスサーバＮＡＳ，そして端末ＴＥへ認証応答を送信するとともに、ユーザ名「ｕｓ０００２」およびパスワード「ｐｓ００００２」を認証情報保持手段２に認証済みユーザ情報とし

て保持する様子を示す。

【0031】次に、データベースDB内の認証情報が変更された場合には、図8に示すように、認証サーバATSは、認証情報変更通知手段1により、ネットワークアクセスサーバNASに認証情報変更通知を送出する。認証情報変更通知を受信したネットワークアクセスサーバNASは、ユーザ情報削除手段4により、通知されたユーザ名に対応する認証済みユーザ情報を認証情報保持手段2から削除する。図8では、データベースDB内の認証情報中、ユーザ名「us0007」のパスワードが「ps0007」から「777777」に変更されたため、認証情報保持手段2中の対応する認証済みユーザ情報であるユーザ名「us0002」および変更前のパスワード「ps0007」を削除した様子が示されている。

【0032】なお、以上に説明した実施例では、データベースDB内の認証情報が変更になった場合、認証サーバATSは認証情報変更通知手段により、変更になったユーザ名をネットワークアクセスサーバNASに通知し、これを受信したネットワークアクセスサーバNASはユーザ情報削除手段4により、保持している認証済みユーザ情報から、通知されたユーザの情報を削除するが、認証サーバATSからの認証情報変更通知で、変更になったユーザの変更情報をネットワークアクセスサーバNASへ通知し、これを受け取ったネットワークアクセスサーバNASが、保持している認証済みユーザ認証情報の指定されたユーザ情報を、認証情報変更通知で通知された内容に更新するようにしてもよい。そのような実施例においては、図8において、認証済みユーザ情報であるユーザ名「us0002」およびパスワード「ps0007」は削除されることはなく、パスワードが「777777」に変更されることとなる。

【0033】また、先の実施例ではネットワークアクセスサーバNASにおける認証済みユーザ情報の保持の条件に関して限定していなかったが、ネットワークアクセスサーバNASのメモリの状態、処理速度への影響等を考慮して、一定期間情報を保持し、その期間内に認証要求を受け取らなかった場合には認証済みユーザ情報は破棄する、もしくは、一定件数の情報を保持したら、それ以降の認証済みユーザ情報を保持する前に古い認証済みユーザ情報を順に破棄するなどして、処理能力の低下を回避するような実施例も考えられる。

【0034】

【発明の効果】本発明によれば、端末がネットワークアクセスサーバへ認証要求を送信した場合、ネットワークアクセスサーバ内の認証済みユーザ情報に保持されているユーザに関しては、ネットワークアクセスサーバ内で認証されるため、認証要求を認証サーバに送信する必要が無くなり、認証サーバの負荷が低減される。また、ネットワークアクセスサーバと認証サーバ間のトラヒックも低減される。

【0035】また、認証サーバの負荷が低減されるため、認証サーバをシステムで多数設置する必要がなく、さらに、端末側では一度認証されたか否かの意識も不要であるため、システム構成が簡略化され、データベース管理も簡略化され運用コストが削減される。

【図面の簡単な説明】

【図1】本発明の一実施例を示すブロック図

【図2】図1に示した実施例のフローチャート

【図3】図2のS2におけるNAS内認証の詳細フローチャート

【図4】図2のS2におけるNAS内認証の結果が「認証」である場合の具体例を示す図

【図5】図2のS2におけるNAS内認証の結果が「認証拒否」である場合の具体例を示す図

【図6】図2のS2におけるNAS内認証の結果が「ユーザ名無し」である場合の具体例を示す図

【図7】図2のS5により認証要求送出をした場合の様子を示す図

【図8】図1のデータベース中の認証情報が変更された場合の様子を示す図

【図9】従来の第1の例を示すブロック図

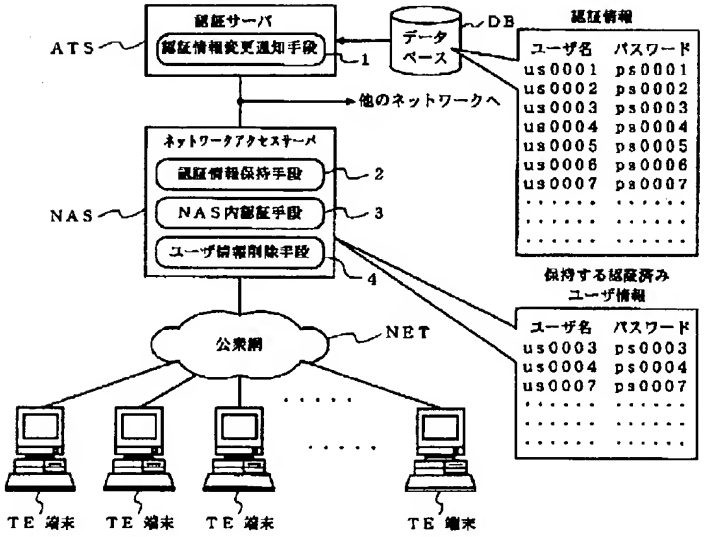
【図10】従来の第2の例を示すブロック図

【図11】本発明と関連する公知技術を示すブロック図

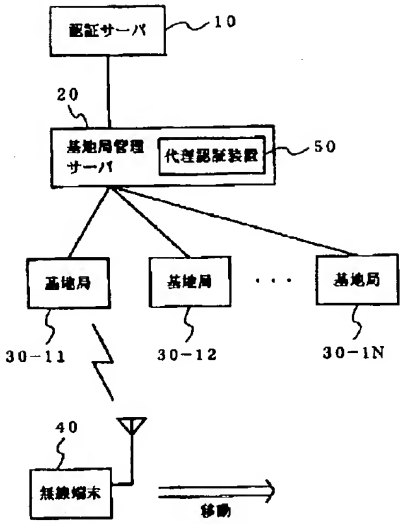
【符号の説明】

ATS，ATS1，10　認証サーバ
NAS，NAS1　ネットワークアクセスサーバ
NET　公衆網
TE　端末
DB　データベース
1　認証情報変更通知手段
2　認証情報保持手段
3　NAS内認証手段
4　ユーザ情報削除手段
20　基地局管理サーバ
30-11，30-12，30-1N　基地局
40　無線端末
50　代理認証装置

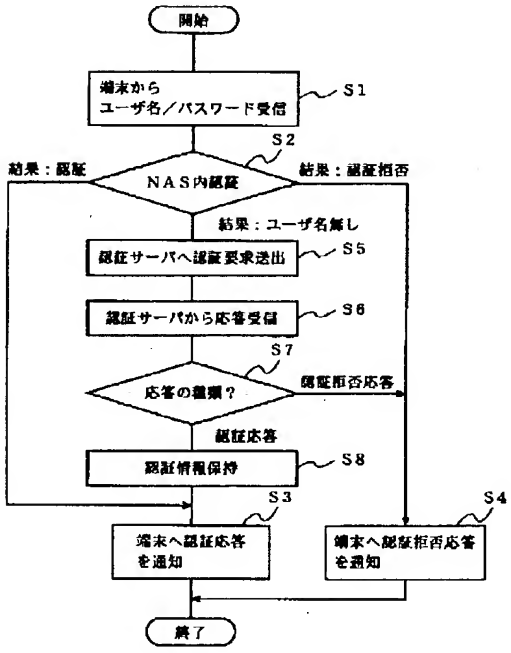
【図１】


認証サーバ
認証情報変更通知手段
1
ATS
データベース
DB
認証情報
ユーザ名　パスワード
us0001　ps0001
us0002　ps0002
us0003　ps0003
us0004　ps0004
us0005　ps0005
us0006　ps0006
us0007　ps0007
他のネットワークへ
ネットワークアクセスサーバ
認証情報保持手段
2
NAS
NAS内認証手段
3
ユーザ情報削除手段
4
保持する認証済み
ユーザ情報
ユーザ名　パスワード
us0003　ps0003
us0004　ps0004
us0007　ps0007
公衆網
NET
TE 端末
TE 端末
TE 端末
TE 端末

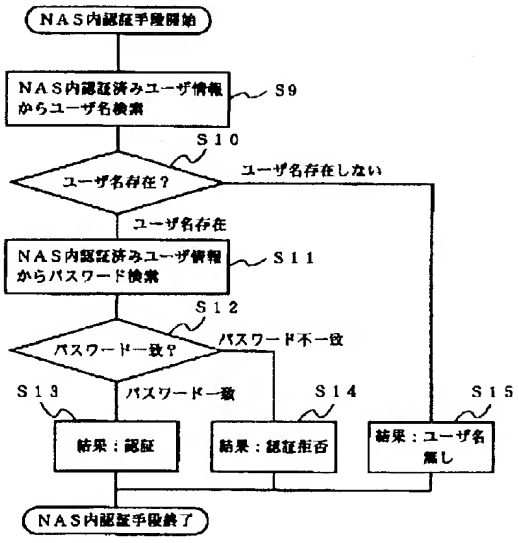
【図１１】


認証サーバ
10
20
基地局管理サーバ
代理認証装置
50
基地局
基地局
基地局
30-11
30-12
30-1N
40
無線端末
移動

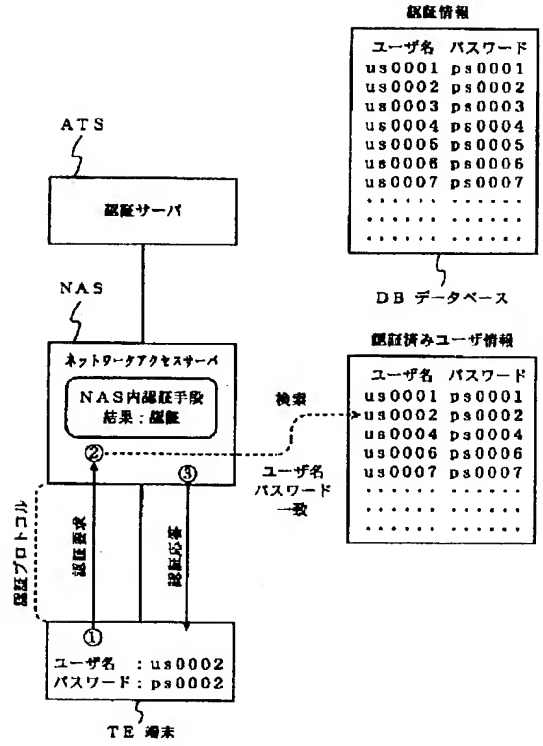
【図２】


開始
端末から
ユーザ名／パスワード受信
S1
S2
結果：認証
NAS内認証
結果：認証拒否
結果：ユーザ名無し
認証サーバへ認証要求送出
S5
認証サーバから応答受信
S6
S7
応答の種類？
認証拒否応答
認証応答
認証情報保持
S8
S3
S4
端末へ認証応答を通知
端末へ認証拒否応答を通知
終了

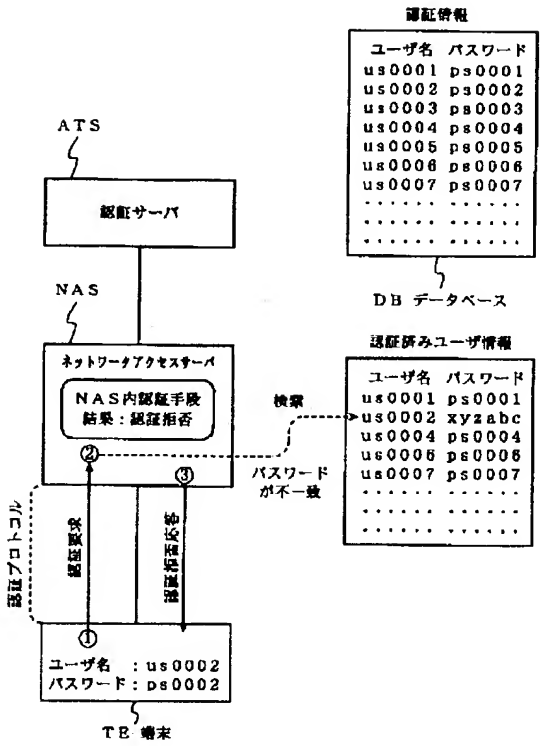
【図３】


NAS内認証手段開始
NAS内認証済みユーザ情報からユーザ名検索
S9
S10
ユーザ名存在？
ユーザ名存在しない
ユーザ名存在
NAS内認証済みユーザ情報からパスワード検索
S11
S12
パスワード一致？
パスワード不一致
S13
パスワード一致
S14
S15
結果：認証
結果：認証拒否
結果：ユーザ名無し
NAS内認証手段終了

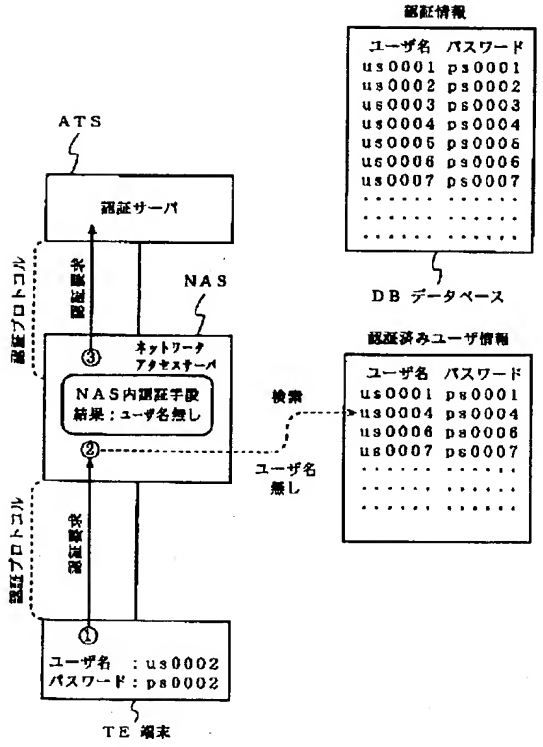
【図4】


認証情報
ユーザ名 パスワード
us0001 ps0001
us0002 ps0002
us0003 ps0003
us0004 ps0004
us0005 ps0005
us0006 ps0006
us0007 ps0007
DB データベース
ATS
認証サーバ
NAS
ネットワークアクセスサーバ
NAS内認証手段
結果：認証
検索
認証済みユーザ情報
ユーザ名 パスワード
us0001 ps0001
us0002 ps0002
us0004 ps0004
us0006 ps0006
us0007 ps0007
ユーザ名
パスワード
一致
認証プロトコル
認証要求
認証応答
①
②
③
ユーザ名 ：us0002
パスワード：ps0002
TE 端末

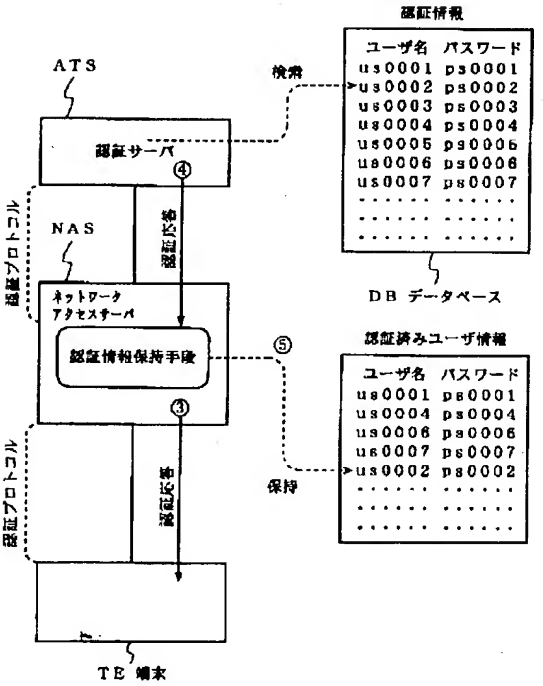
【図5】


認証情報
ユーザ名 パスワード
us0001 ps0001
us0002 ps0002
us0003 ps0003
us0004 ps0004
us0005 ps0005
us0006 ps0006
us0007 ps0007
DB データベース
ATS
認証サーバ
NAS
ネットワークアクセスサーバ
NAS内認証手段
結果：認証拒否
検索
認証済みユーザ情報
ユーザ名 パスワード
us0001 ps0001
us0002 xyzabc
us0004 ps0004
us0006 ps0006
us0007 ps0007
パスワード
が不一致
認証プロトコル
認証要求
認証拒否応答
①
②
③
ユーザ名 ：us0002
パスワード：ps0002
TE 端末

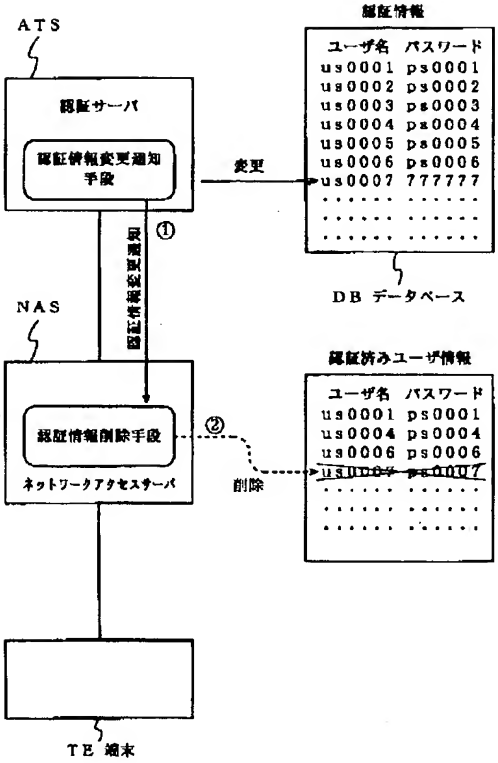
【図6】


認証情報
ユーザ名 パスワード
us0001 ps0001
us0002 ps0002
us0003 ps0003
us0004 ps0004
us0005 ps0006
us0006 ps0006
us0007 ps0007
DB データベース
ATS
認証サーバ
認証プロトコル
認証要求
NAS
ネットワーク
アクセスサーバ
NAS内認証手段
結果：ユーザ名無し
検索
認証済みユーザ情報
ユーザ名 パスワード
us0001 ps0001
us0004 ps0004
us0006 ps0006
us0007 ps0007
ユーザ名
無し
①
②
③
ユーザ名 ：us0002
パスワード：ps0002
TE 端末

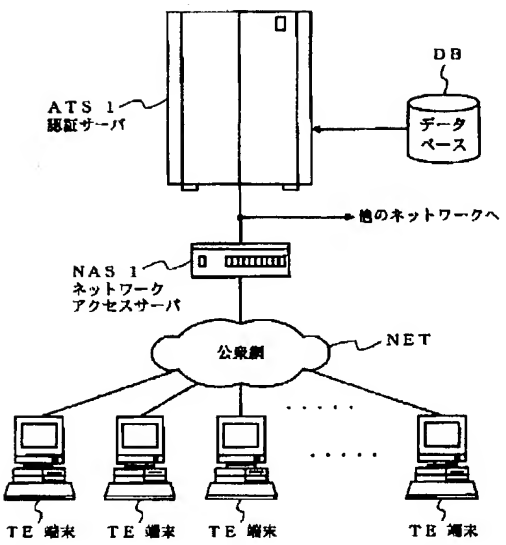
【図7】


認証情報
ユーザ名 パスワード
us0001 ps0001
us0002 ps0002
us0003 ps0003
us0004 ps0004
us0005 ps0006
us0006 ps0006
us0007 ps0007
DB データベース
ATS
検索
認証サーバ
④
認証応答
NAS
ネットワーク
アクセスサーバ
認証情報保持手段
⑤
保持
③
認証応答
認証プロトコル
認証済みユーザ情報
ユーザ名 パスワード
us0001 ps0001
us0004 ps0004
us0006 ps0006
us0007 ps0007
us0002 ps0002
TE 端末

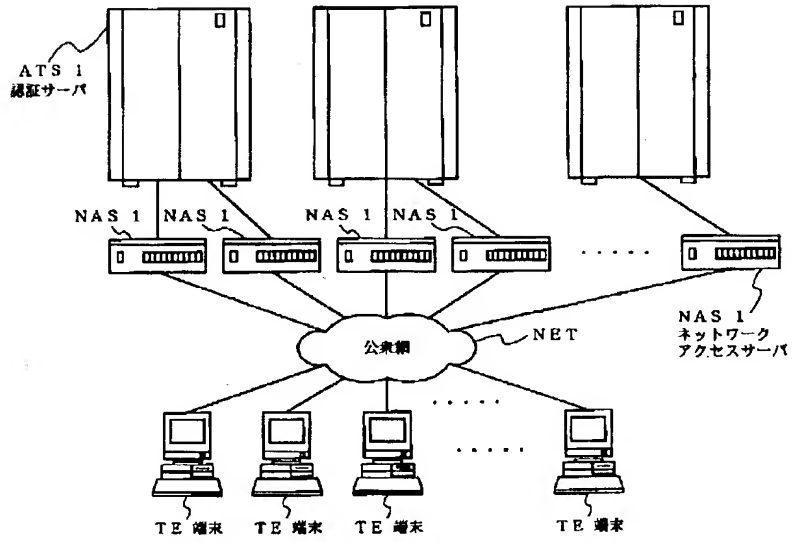
【図8】


ATS
認証サーバ
認証情報変更通知手段
変更
認証情報
ユーザ名 パスワード
us0001 ps0001
us0002 ps0002
us0003 ps0003
us0004 ps0004
us0005 ps0005
us0006 ps0006
us0007 777777
DB データベース
①
認証情報変更通知
NAS
認証情報削除手段
②
削除
ネットワークアクセスサーバ
認証済みユーザ情報
ユーザ名 パスワード
us0001 ps0001
us0004 ps0004
us0006 ps0006
us0007 ps0007
TE 端末

【図9】


ATS 1
認証サーバ
DB
データベース
他のネットワークへ
NAS 1
ネットワーク
アクセスサーバ
公衆網
NET
TE 端末
TE 端末
TE 端末
TE 端末

【図10】


ATS 1
認証サーバ
NAS 1
NAS 1
NAS 1
NAS 1
公衆網
NET
NAS 1
ネットワーク
アクセスサーバ
TE 端末
TE 端末
TE 端末
TE 端末